

An infinite family of strongly unextendible mutually unbiased bases in \mathbb{C}^{2^h}

Jonathan Jedwab

Lily Yen

16 April 2016

Abstract

A set of b mutually unbiased bases (MUBs) in \mathbb{C}^d (for $d > 1$) comprises bd vectors in \mathbb{C}^d , partitioned into b orthogonal bases for \mathbb{C}^d such that the pairwise angle between all vectors from distinct bases is $\arccos(1/\sqrt{d})$. The largest number $\mu(d)$ of MUBs that can exist in \mathbb{C}^d is at most $d + 1$, but constructions attaining this bound are known only when d is a prime power. A set of b MUBs in \mathbb{C}^d that cannot be enlarged, even by the first vector of a potential $(b + 1)$ -th MUB, is called strongly unextendible. Until now, only one infinite family of dimensions d containing $b(d)$ strongly unextendible MUBs in \mathbb{C}^d satisfying $b(d) < \mu(d)$ was known; this family, due to Szántó, is asymptotically “large” in the sense that $b(d)/\mu(d) \rightarrow 1$ as $d \rightarrow \infty$. However, the existence of $2^{m-1} + 1$ strongly unextendible MUBs in \mathbb{C}^{2^m} for each integer $m > 1$ has been conjectured by Mandayam et al. We prove their conjecture for all even values of m , using only elementary linear algebra. The existence of this “small” new infinite family suggests, contrary to widespread belief, that $\mu(d)$ for non-prime-powers d might be significantly larger than the size of particular unextendible sets.

1 Introduction

The Hermitian inner product of vectors $A = (A(x))_{0 \leq x < d}$ and $B = (B(x))_{0 \leq x < d}$ in \mathbb{C}^d is $\langle A, B \rangle = \sum_{x=0}^{d-1} A(x)\overline{B(x)}$. The *angle* between A and B is $\arccos(\frac{|\langle A, B \rangle|}{\|A\| \cdot \|B\|})$, where $\|A\| = \sqrt{\langle A, A \rangle}$ is the norm of A . A set of b *mutually unbiased bases* (MUBs) in \mathbb{C}^d (for $d > 1$) comprises bd vectors in \mathbb{C}^d , partitioned into b orthogonal bases for \mathbb{C}^d such that the pairwise angle between vectors in distinct bases is $\arccos(1/\sqrt{d})$. After applying a unitary transformation and normalizing, we may assume that one of the bases is \sqrt{d} times the standard basis and therefore that each component of each vector in all other bases has unit magnitude. The angle condition for these other bases is

J. Jedwab is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada.

L. Yen is with Department of Mathematics and Statistics, Capilano University, 2055 Purcell Way, North Vancouver BC V7J 3H5, Canada and Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada.

J. Jedwab is supported by NSERC.

Email: jed@sfu.ca, lyen@capilanou.ca

2010 Mathematics Subject Classification 05B20, 15A30, 81P45, 94B60

then $|\langle A, B \rangle| = \sqrt{d}$ for vectors A, B in distinct bases. For example, the following sets of vectors form 5 MUBs in \mathbb{C}^4 :

$$\begin{array}{ccccc} (2 & 0 & 0 & 0) & (1 & 1 & 1 & 1) & (1 & 1 & i & -i) & (1 & i & 1 & -i) & (1 & i & i & -1) \\ (0 & 2 & 0 & 0) & (1 & 1 & -1 & -1) & (1 & 1 & -i & i) & (1 & i & -1 & i) & (1 & i & -i & 1) \\ (0 & 0 & 2 & 0) & (1 & -1 & 1 & -1) & (1 & -1 & i & i) & (1 & -i & 1 & i) & (1 & -i & i & 1) \\ (0 & 0 & 0 & 2) & (1 & -1 & -1 & 1) & (1 & -1 & -i & -i) & (1 & -i & -1 & -i) & (1 & -i & -i & -1) \end{array}$$

Schwinger [Sch60] introduced MUBs in 1960, noting that when a quantum system is prepared in a state belonging to one basis, all outcomes of measurement with respect to any other basis are equally probable and therefore convey no information about the system. The term “mutually unbiased bases” was introduced by Wootters and Fields in 1989 [WF89]. The MUB property can be exploited in secure quantum key exchange [BB14], quantum state determination [Iva81], quantum state reconstruction [WF89], and detection of quantum entanglement [SHB⁺12]; see [DEBZ10] for a comprehensive survey of research on MUBs up to 2010. There are intriguing connections between MUBs and various combinatorial structures, including finite projective planes [SPR04], mutually orthogonal Latin squares [WB05], relative difference sets [GR09], complex Hadamard matrices [Szö11], and complex equiangular lines [JW].

The central problem is to determine the largest number $\mu(d)$ of MUBs that can exist in \mathbb{C}^d . Following Grassl [Gra09], we call a set of b MUBs in \mathbb{C}^d that cannot be enlarged to a set of size $b + 1$ MUBs \mathbb{C} -*unextendible*, and a set that cannot be enlarged by even one vector of a potential $(b + 1)$ -th MUB *strongly* \mathbb{C} -*unextendible*; in the latter case, we say there is no vector in \mathbb{C} that is unbiased with respect to each vector of the MUBs. Corresponding definitions apply for MUBs in \mathbb{R}^d and for (strongly) \mathbb{R} -unextendible sets.

More than forty years ago, Delsarte, Goethals, and Seidel [DGS75] used Jacobi polynomials to establish an upper bound on $\mu(d)$ and on the corresponding quantity for MUBs in \mathbb{R}^d .

Theorem 1. [DGS75, Table I with $\alpha = 1/d$ and $\beta = 0$]

- (i) *The number $\mu(d)$ of MUBs that can exist in \mathbb{C}^d is at most $d + 1$. Every set of $d + 1$ MUBs in \mathbb{C}^d is strongly \mathbb{C} -unextendible.*
- (ii) *The number of MUBs that can exist in \mathbb{R}^d is at most $d/2 + 1$. Every set of $d/2 + 1$ MUBs in \mathbb{R}^d is strongly \mathbb{R} -unextendible.*

The following lower bound on $\mu(d)$, arising from a product construction, is due to Klappenecker and Rötteler [KR04].

Theorem 2. [KR04, Lemma 3] *Let $d, d' > 1$. Then $\mu(dd') \geq \min(\mu(d), \mu(d'))$.*

The upper bound $d + 1$ on $\mu(d)$ in Theorem 1 (i) is attained when d is a prime power [Iva81], [WF89]. It follows from Theorem 2 that, for distinct primes p_1, p_2, \dots, p_r and positive integers a_1, a_2, \dots, a_r , we have $\mu(p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}) \geq 1 + \min_i p_i^{a_i}$; a stronger lower bound can be obtained for infinitely many dimensions using sets of mutually orthogonal Latin squares [WB05]. However, it is not known whether the upper bound on $\mu(d)$ in Theorem 1 (i) is attained for even a single value of $d > 1$ that is not a prime power. Indeed, the determination of $\mu(d)$ for non-prime-powers d was proposed in 2006 as one of *The ten most annoying questions in quantum computing* (by virtue of having “caused all would-be climbers to fall flat on their asses”!) [Aar06]; in 2014, only this question and two others from the original list remained unanswered [Aar14]. It is therefore

interesting to pose the question: When and how can a set of MUBs be extended and, if it cannot, then when and why is it strongly unextendible? We now summarise the few known general results addressing this question.

Theorem 3. [Wei13] *Every set of d MUBs in \mathbb{C}^d is extendible to a set of $d + 1$ MUBs in \mathbb{C}^d (that is, $\mu(d) \neq d$).*

In view of Theorems 1, 2, 3, the current state of knowledge for the smallest non-prime-power dimension 6 is that $\mu(6) \in \{3, 4, 5, 7\}$. Several constructions of infinite families of sets of 3 MUBs in \mathbb{C}^6 are known [Zau99, p. 57], [JMM⁺09, Appendix B], [Szö10], but no set of 4 MUBs in \mathbb{C}^6 has been found. Indeed, Zauner [Zau99, p. 57] conjectured in 1999 that no such set exists. In 2007, Bengtsson [Ben07] reported “a growing consensus” in favour of this conjecture, yet concluded that “We have almost no evidence either way”. Three years later, Durt et al. [DEBZ10] considered that “the evidence for [Zauner’s] conjecture is overwhelming, but not quite conclusive”. Two pieces of supporting evidence for the conjecture are: a computational proof that if at least one of a set of 3 MUBs in \mathbb{C}^6 is constrained to belong to the “Fourier family $F(a, b)$ ” (a generalization of the Fourier matrix of order 6) then the set is \mathbb{C} -unextendible [JMM⁺09]; and a proof that every set of 3 MUBs in \mathbb{C}^6 arising from the product construction leading to Theorem 2 is strongly \mathbb{C} -unextendible [MW12].

Until now, only one infinite family of dimensions d containing $b(d)$ strongly unextendible MUBs in \mathbb{C}^d satisfying $b(d) < \mu(d)$ was known, due to Szántó.

Theorem 4. [Szál16] *For each prime p congruent to 3 modulo 4, there exists a set of $p^2 - p + 2$ strongly \mathbb{C} -unextendible MUBs in \mathbb{C}^{p^2} . For $p = 2, 3, 5, 7, 11$ there also exists a set of $p^2 - 1$ strongly \mathbb{C} -unextendible MUBs in \mathbb{C}^{p^2} .*

The motivation for this paper is provided by two sets of strongly \mathbb{C} -unextendible MUBs and an accompanying conjecture recently presented by Mandayam et al. [MBGW14].

Theorem 5. [MBGW14, Section 4] *There exist 3 strongly \mathbb{C} -unextendible MUBs in \mathbb{C}^4 , and 5 strongly \mathbb{C} -unextendible MUBs in \mathbb{C}^8 .*

Conjecture 6. [MBGW14, Conjecture 1] *For each integer $m > 1$, there exists a set of $2^{m-1} + 1$ strongly \mathbb{C} -unextendible MUBs in \mathbb{C}^{2^m} .*

Strong \mathbb{C} -unextendibility in Theorem 5 was verified computationally in [MBGW14], using Gröbner basis techniques. The sets of MUBs in Theorem 5 were constructed from maximal commuting classes of Pauli operators, and Conjecture 6 was stated in [MBGW14] as holding specifically for such sets. K. Thas [Tha] subsequently showed that Conjecture 6 is false for all $m > 3$ when this restriction is applied, but proposed that the conjecture holds for all $m > 1$ using MUBs constructed from complete partial spreads [Tha, Conjecture 8.6].

The main result of this paper is Theorem 7, which establishes Conjecture 6 (without reference to complete partial spreads) for all even m .

Theorem 7. *For each integer $h \geq 1$, there exists a set of $2^{2h-1} + 1$ strongly \mathbb{C} -unextendible MUBs in $\mathbb{C}^{2^{2h}}$.*

Our proof of Theorem 7 uses only elementary linear algebra, and does not rely at all on computation. We specify the sets of MUBs described in Theorem 7 explicitly; in fact, they are MUBs in $\{1, -1\}^{2^{2h}}$ that have long been known to attain the upper bound of Theorem 1 (ii) when d

is a power of 4 (see Proposition 8 and Theorem 9). The new and surprising result is that these MUBs, which are strongly \mathbb{R} -unextendible by Theorem 1 (ii), are also strongly \mathbb{C} -unextendible. Theorem 7 gives the first known infinite family of $b(d)$ strongly \mathbb{C} -unextendible MUBs in \mathbb{C}^d for which $\lim_{d \rightarrow \infty} b(d)/\mu(d) < 1$. The existence of this family suggests that caution is warranted, for example, in interpreting the existence of sets of 3 \mathbb{C} -unextendible MUBs in \mathbb{C}^6 [JMM⁺09], [MW12] as evidence that $\mu(6) < 7$, especially when the sets are constrained to satisfy some structural condition; indeed, we see that for $d = 2^{2h}$ there exist sets of $d/2 + 1$ strongly \mathbb{C} -unextendible MUBs in \mathbb{C}^d (constrained actually to lie in \mathbb{R}^d) even though $\mu(d) = d + 1$.

In Section 2, we shall provide required background on Boolean functions and bent functions, including short proofs of some known results with the intention of making the paper more accessible. In Section 3, we shall prove Theorem 7.

2 Boolean functions and bent functions

A *Boolean function* on \mathbb{Z}_2^m is a function $g : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2$. The corresponding vector $(g(x))_{x \in \mathbb{Z}_2^m} \in \mathbb{Z}_2^{2^m}$ is the evaluation of $g(x)$ at the 2^m points of \mathbb{Z}_2^m taken in lexicographic order. For example, the vector corresponding to the Boolean function $g(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_4$ on \mathbb{Z}_2^4 is (0000010100111001), whose initial element is $g(0, 0, 0, 0)$ and whose final element is $g(1, 1, 1, 1)$. See [Car10] and [CM16], for example, for detailed background on Boolean functions.

The *Walsh-Hadamard transform* of a Boolean function g on \mathbb{Z}_2^m is the function $\hat{g} : \mathbb{Z}_2^m \rightarrow \mathbb{Z}$ given by

$$\hat{g}(u) = \sum_{x \in \mathbb{Z}_2^m} (-1)^{g(x) + u \cdot x} \quad \text{for } u \in \mathbb{Z}_2^m,$$

where \cdot is the usual inner product in \mathbb{Z}_2^m . A Boolean function g on \mathbb{Z}_2^m is *bent* if

$$\hat{g}(u) \in \{2^{m/2}, -2^{m/2}\} \quad \text{for all } u \in \mathbb{Z}_2^m.$$

Bent functions exist for all positive even integers m .

A *bent set* on \mathbb{Z}_2^{2h} is a finite set of Boolean functions on \mathbb{Z}_2^{2h} for which the sum of any two distinct functions in the set is bent. We may assume (by adding one function to all the others) that one element of the set is the zero function, and then all the other elements are themselves bent. For example, a bent set of size 8 on \mathbb{Z}_2^4 is given by the Boolean functions

$$0, \quad x_1x_2 + x_3x_4, \quad x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3, \quad x_1x_2 + x_1x_3 + x_2x_4, \quad x_1x_2 + x_1x_4 + x_2x_3 + x_2x_4, \\ x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4, \quad x_1x_3 + x_2x_3 + x_2x_4 + x_3x_4, \quad x_1x_4 + x_2x_3 + x_3x_4.$$

A bent set on \mathbb{Z}_2^{2h} can be used to construct a set of real MUBs in $\{1, -1\}^{2^{2h}}$, as we now describe. Write $I[\cdot]$ for the indicator function.

Proposition 8. [CS73] (see also [CCKS97], [Kan95]) *Suppose $\{g_1, g_2, \dots, g_r\}$ is a bent set on \mathbb{Z}_2^{2h} . Then 2^h times the standard basis for $\mathbb{R}^{2^{2h}}$, together with the r sets of 2^{2h} vectors $\{((-1)^{g_j(x) + u \cdot x})_{x \in \mathbb{Z}_2^{2h}} : u \in \mathbb{Z}_2^{2h}\}$ for $1 \leq j \leq r$, form $r + 1$ MUBs in $\{1, -1\}^{2^{2h}}$.*

Proof. For each j , the 2^{2h} vectors of $B_j = \{((-1)^{g_j(x) + u \cdot x})_{x \in \mathbb{Z}_2^{2h}} : u \in \mathbb{Z}_2^{2h}\}$ form an orthogonal basis for $\mathbb{R}^{2^{2h}}$, because for distinct $u, v \in \mathbb{Z}_2^{2h}$ we have

$$\left\langle ((-1)^{g_j(x) + u \cdot x})_x, ((-1)^{g_j(x) + v \cdot x})_x \right\rangle = \sum_{x \in \mathbb{Z}_2^{2h}} (-1)^{(u+v) \cdot x} = 0$$

using the identity

$$\sum_{w \in \mathbb{Z}_2^m} (-1)^{w \cdot z} = 2^m I[z = 0] \quad \text{for all } z \in \mathbb{Z}_2^m. \quad (1)$$

The vectors from distinct bases B_j and B_k are mutually unbiased, because for $u, v \in \mathbb{Z}_2^{2h}$ we have

$$\left\langle ((-1)^{g_j(x)+u \cdot x})_x, ((-1)^{g_k(x)+v \cdot x})_x \right\rangle = \sum_{x \in \mathbb{Z}_2^{2h}} (-1)^{(g_j+g_k)(x)+(u+v) \cdot x} = \widehat{g_j + g_k}(u + v),$$

which has magnitude $\sqrt{2^{2h}}$ because $g_j + g_k$ is a bent function on \mathbb{Z}_2^{2h} for distinct j, k . \square

The following existence result for bent sets is due to Kerdock [Ker72].

Theorem 9. [Ker72], [MS86, p. 456] *For each integer $h \geq 1$, there exists a bent set of size 2^{2h-1} on \mathbb{Z}_2^{2h} .*

Application of Proposition 8 to the bent set of Theorem 9 produces a set of $2^{2h-1} + 1$ MUBS in $\{1, -1\}^{2^{2h}}$, which attains the upper bound in Theorem 1 (ii) for the number of MUBs in \mathbb{R}^d when $d = 2^{2h}$.

We require two further auxiliary results. Write $(\mathbb{Z}_2^m)^*$ for $\mathbb{Z}_2^m \setminus \{0\}$.

Proposition 10. [Car10, p.79] *Suppose $g(x)$ is a bent function on \mathbb{Z}_2^{2h} , and let $a \in (\mathbb{Z}_2^{2h})^*$. Then*

$$\sum_{x \in \mathbb{Z}_2^{2h}} (-1)^{g(x)+g(x+a)} = 0.$$

Proof. Since $g(x)$ is bent, we have

$$2^{2h} = |\hat{g}(u)|^2 = \sum_{x, y \in \mathbb{Z}_2^{2h}} (-1)^{g(x)+u \cdot x} (-1)^{g(y)+u \cdot y} = \sum_{x, b \in \mathbb{Z}_2^{2h}} (-1)^{g(x)+g(x+b)} (-1)^{u \cdot b}$$

by setting $y = x + b$. Multiply the first and last expressions by $(-1)^{u \cdot a}$ and sum over $u \in \mathbb{Z}_2^{2h}$ to give

$$2^{2h} \sum_{u \in \mathbb{Z}_2^{2h}} (-1)^{u \cdot a} = \sum_{x, b \in \mathbb{Z}_2^{2h}} (-1)^{g(x)+g(x+b)} \sum_{u \in \mathbb{Z}_2^{2h}} (-1)^{u \cdot (a+b)}.$$

The result follows by applying (1) to the sum over u on both sides. \square

Lemma 11. *The 2^m vectors $\{((-1)^{u \cdot \ell})_{u \in \mathbb{Z}_2^m} : \ell \in \mathbb{Z}_2^m\}$ are pairwise orthogonal, and therefore linearly independent over \mathbb{R} .*

Proof. For distinct $k, \ell \in \mathbb{Z}_2^m$, we have $\langle ((-1)^{u \cdot k})_u, ((-1)^{u \cdot \ell})_u \rangle = \sum_{u \in \mathbb{Z}_2^m} (-1)^{u \cdot (k+\ell)} = 0$ by (1). \square

3 Proof of Theorem 7

Proof of Theorem 7. From Theorem 9, there exists a bent set $\{g_1, g_2, \dots, g_{2^{2h}-1}\}$ on \mathbb{Z}_2^{2h} and we may assume $g_1 = 0$. From Proposition 8, this bent set gives a set of $2^{2h-1} + 1$ MUBs in $\{1, -1\}^{2^{2h}}$, comprising 2^h times the standard basis together with the 2^{2h-1} bases $\{((-1)^{g_j(x)+u \cdot x})_{x \in \mathbb{Z}_2^{2h}} : u \in \mathbb{Z}_2^{2h}\}$ for $1 \leq j \leq 2^{2h-1}$. We shall show that these MUBs are strongly \mathbb{C} -unextendible.

Suppose, for a contradiction, that the vector $(A(x))_{x \in \mathbb{Z}_2^{2h}} \in \mathbb{C}^{2^{2h}}$ is unbiased with respect to each vector of these MUBs. By reference to 2^h times the standard basis, each $A(x)$ has magnitude 1. By reference to the other 2^{2h-1} bases, for $1 \leq j \leq 2^{2h-1}$ and $u \in \mathbb{Z}_2^{2h}$ we have

$$\left| \sum_{x \in \mathbb{Z}_2^{2h}} A(x) (-1)^{g_j(x)+u \cdot x} \right| = 2^h$$

and squaring yields

$$\sum_{x, y \in \mathbb{Z}_2^{2h}} A(x) \overline{A(y)} (-1)^{g_j(x)+g_j(y)+u \cdot (x+y)} = 2^{2h}.$$

The terms of this sum for which $x = y$ contribute $\sum_{x \in \mathbb{Z}_2^{2h}} |A(x)|^2 = \sum_{x \in \mathbb{Z}_2^{2h}} 1 = 2^{2h}$, and therefore

$$\sum_{\substack{x, y \in \mathbb{Z}_2^{2h} \\ x \neq y}} A(x) \overline{A(y)} (-1)^{g_j(x)+g_j(y)+u \cdot (x+y)} = 0 \quad \text{for } 1 \leq j \leq 2^{2h-1} \text{ and } u \in \mathbb{Z}_2^{2h}. \quad (2)$$

Order the elements of \mathbb{Z}_2^{2h} lexicographically, writing $x < y$ to mean that x precedes y in this ordering. Define

$$a_{x,y} = \frac{1}{2} \left(A(x) \overline{A(y)} + A(y) \overline{A(x)} \right) = \operatorname{Re} \left(A(x) \overline{A(y)} \right) \quad \text{for } x, y \in \mathbb{Z}_2^{2h}$$

and

$$m_{j,u,x,y} = (-1)^{g_j(x)+g_j(y)+u \cdot (x+y)}$$

Then from (2) we have

$$\sum_{\substack{x, y \in \mathbb{Z}_2^{2h} \\ x < y}} m_{j,u,x,y} a_{x,y} = 0 \quad \text{for } 1 \leq j \leq 2^{2h-1} \text{ and } u \in \mathbb{Z}_2^{2h},$$

which is a homogeneous linear system of $2^{2h-1} \cdot 2^{2h} = 2^{4h-1}$ equations in the $\binom{2^{2h}}{2} = 2^{2h-1}(2^{2h}-1)$ real variables $(a_{x,y})_{x < y}$. We can represent this system in the form $M\mathbf{a} = \mathbf{0}$ where $M = (m_{j,u,x,y})$ is the $2^{4h-1} \times 2^{2h-1}(2^{2h}-1)$ real matrix whose rows are indexed by (j, u) and whose columns are indexed by (x, y) with $x < y$, and $\mathbf{a} = (a_{x,y})_{x < y}$ is a vector of $2^{2h-1}(2^{2h}-1)$ real entries.

Partition the columns of M into $2^{2h}-1$ submatrices M_ℓ of size $2^{4h-1} \times 2^{2h-1}$, where M_ℓ is given by

$$M_\ell = (m_{j,u,x,\ell+x}) = ((-1)^{g_j(x)+g_j(\ell+x)+u \cdot \ell}) \quad \text{for } \ell \in (\mathbb{Z}_2^{2h})^*.$$

The rows of M_ℓ are indexed by (j, u) , and the columns are indexed by $(x, \ell+x)$ for the 2^{2h-1} values of $x \in \mathbb{Z}_2^{2h}$ satisfying $x < \ell+x$.

For each $\ell \in (\mathbb{Z}_2^{2h})^*$, the first 2^{2h} entries of each column of M_ℓ are given by the vector $(m_{1,u,x,\ell+x})_{u \in \mathbb{Z}_2^{2h}} = ((-1)^{u \cdot \ell})_{u \in \mathbb{Z}_2^{2h}}$ (independently of x), using $g_1 = 0$. The set of all $2^{2h} - 1$ such vectors, as ℓ ranges over $(\mathbb{Z}_2^{2h})^*$, is linearly independent over \mathbb{R} by Lemma 11, and therefore

$$\text{rank}(M) = \sum_{\ell \in (\mathbb{Z}_2^{2h})^*} \text{rank}(M_\ell).$$

We claim that

$$\text{rank}(M_\ell) = 2^{2h-1} \quad \text{for each } \ell \in (\mathbb{Z}_2^{2h})^*.$$

It then follows that $\text{rank}(M) = 2^{2h-1}(2^{2h} - 1)$, so M has full rank. The homogeneous linear system $M\mathbf{a} = \mathbf{0}$ therefore has only the trivial solution

$$a_{x,y} = 0 \quad \text{for all } x < y.$$

Writing $A(x) = e^{i\theta(x)}$ (using that each $A(x)$ has magnitude 1), this implies by the definition of $a_{x,y}$ that $\cos(\theta(x) - \theta(y)) = 0$ for all $x < y$. This is possible only if the vector $(A(x))$ contains at most 2 entries, which contradicts that the vector $(A(x))$ contains $2^{2h} \geq 4$ entries.

To prove the claim we note that, for $\ell \in (\mathbb{Z}_2^{2h})^*$, the 2^{2h-1} rows of M_ℓ given by

$$(m_{j,0,x,\ell+x})_{x < \ell+x} = \left((-1)^{g_j(x) + g_j(\ell+x)} \right)_{x < \ell+x} \quad \text{for } 1 \leq j \leq 2^{2h-1}$$

are pairwise orthogonal and therefore linearly independent over \mathbb{R} : for distinct j, k we have

$$\begin{aligned} \sum_{x < \ell+x} m_{j,0,x,\ell+x} m_{k,0,x,\ell+x} &= \sum_{\substack{x \in \mathbb{Z}_2^{2h} \\ x < \ell+x}} (-1)^{g_j(x) + g_k(x) + g_j(\ell+x) + g_k(\ell+x)} \\ &= \frac{1}{2} \sum_{x \in \mathbb{Z}_2^{2h}} (-1)^{(g_j + g_k)(x) + (g_j + g_k)(\ell+x)} \\ &= 0 \end{aligned}$$

by Proposition 10, because $g_j + g_k$ is bent and $\ell \in (\mathbb{Z}_2^{2h})^*$. □

References

- [Aar06] S. Aaronson. The ten most annoying questions in quantum computing, August 2006. <http://www.scottaaronson.com/blog/?p=112>.
- [Aar14] S. Aaronson. The NEW ten most annoying questions in quantum computing, May 2014. <http://www.scottaaronson.com/blog/?p=1792>.
- [BB14] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoret. Comput. Sci.*, 560, Part 1:7–11, 2014.
- [Ben07] I. Bengtsson. Three ways to look at mutually unbiased bases. In *Foundations of Probability and Physics — 4*, volume 889 of *AIP Conf. Proc.*, pages 40–51. Amer. Inst. Phys., New York, 2007.

- [Car10] C. Carlet. Boolean functions for cryptography and error correcting codes. In Y. Crama and P.L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, volume 134 of *Encyclopedia Math. and its Applications*, pages 257–397. Cambridge Univ. Press, Cambridge, UK, 2010.
- [CCKS97] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel. \mathbb{Z}_4 -Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. *Proc. London Math. Soc. (3)*, 75(2):436–480, 1997.
- [CM16] C. Carlet and S. Mesnager. Four decades of research on bent functions. *Des. Codes Cryptogr.*, 78(1):5–50, 2016.
- [CS73] P. J. Cameron and J. J. Seidel. Quadratic forms over $GF(2)$. *Nederl. Akad. Wetensch. Proc. Ser. A vol. 76 = Indag. Math.*, 35:1–8, 1973.
- [DEBZ10] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski. On mutually unbiased bases. *Int. J. Quantum. Inf.*, 8:535–640, 2010.
- [DGS75] P. Delsarte, J. M. Goethals, and J. J. Seidel. Bounds for systems of lines, and Jacobi polynomials. *Philips Res. Repts*, 30:91–105, 1975.
- [GR09] C. Godsil and A. Roy. Equiangular lines, mutually unbiased bases, and spin models. *European J. Combin.*, 30(1):246–262, 2009.
- [Gra09] M. Grassl. Unextendible mutually unbiased bases, July 2009. Slide presentation at International Conference on Quantum Foundations and Technology: Frontier and Future, Shanghai, http://quantum.ustc.edu.cn/old/conference/program2009/ppt_file/Markus_Grassl_Grassl_UnextendibleMUBs.pdf.
- [Iva81] I. D. Ivanović. Geometrical description of quantal state determination. *J. Phys. A*, 14(12):3241–3245, 1981.
- [JMM⁺09] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, and M. Weiner. A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6. *J. Phys. A*, 42(24):245305, 25, 2009.
- [JW] J. Jedwab and A. Wiebe. Constructions of complex equiangular lines from mutually unbiased bases. *Des. Codes Cryptogr.* Accepted, 2015. arXiv:1408.5169.
- [Kan95] W.M. Kantor. Codes, quadratic forms and finite geometries. In *Different Aspects of Coding Theory*, volume 50 of *Proc. Symp. Appl. Math.*, pages 153–177. Amer. Math. Soc., 1995.
- [Ker72] A. M. Kerdock. A class of low-rate nonlinear binary codes. *Information and Control*, 20:182–187; *ibid.* 21 (1972), 395, 1972.
- [KR04] A. Klappenecker and M. Rötteler. Constructions of mutually unbiased bases. In *Finite fields and applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, pages 137–144. Springer, Berlin, 2004.

- [MBGW14] P. Mandayam, S. Bandyopadhyay, M. Grassl, and W. Wootters. Unextendible mutually unbiased bases from Pauli classes. *Quantum Inf. Comput.*, 14(9&10):823–844, 2014.
- [MS86] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1986.
- [MW12] D. McNulty and S. Weigert. On the impossibility to extend triples of mutually unbiased product bases in dimension six. *Int. J. Quantum Inf.*, 10(5):1250056, 11, 2012.
- [Sch60] J. Schwinger. Unitary operator bases. *Proc. Nat. Acad. Sci. U.S.A.*, 46:570–579, 1960.
- [SHB⁺12] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B. C. Hiesmayr. Entanglement detection via mutually unbiased bases. *Phys. Rev. A*, 86:022311, Aug 2012.
- [SPR04] M. Saniga, M. Planat, and H. Rosu. Mutually unbiased bases and finite projective planes. *J. Opt. B Quantum Semiclass. Opt.*, 6(9):L19–L20, 2004.
- [Sz16] A. Szántó. Complementary decompositions and unextendible mutually unbiased bases. *Linear Algebra Appl.*, 496:392–406, 2016.
- [Sz10] F. Szöllősi. A two-parameter family of complex Hadamard matrices of order 6 induced by hypocycloids. *Proc. Amer. Math. Soc.*, 138(3):921–928, 2010.
- [Sz11] F. Szöllősi. *Construction, Classification and Parametrization of Complex Hadamard Matrices*. PhD thesis, Central European University, 2011.
- [Tha] K. Thas. Unextendible mutually unbiased bases (after Mandayam, Bandyopadhyay, Grassl and Wootters). arXiv:1407.2778 [quant-ph].
- [WB05] P. Wocjan and T. Beth. New construction of mutually unbiased bases in square dimensions. *Quantum Inf. Comput.*, 5(2):93–101, 2005.
- [Wei13] M. Weiner. A gap for the maximum number of mutually unbiased bases. *Proc. Amer. Math. Soc.*, 141:1963–1969, 2013.
- [WF89] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Ann. Physics*, 191(2):363–381, 1989.
- [Zau99] G. Zauner. *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*. PhD thesis, University of Vienna, 1999.